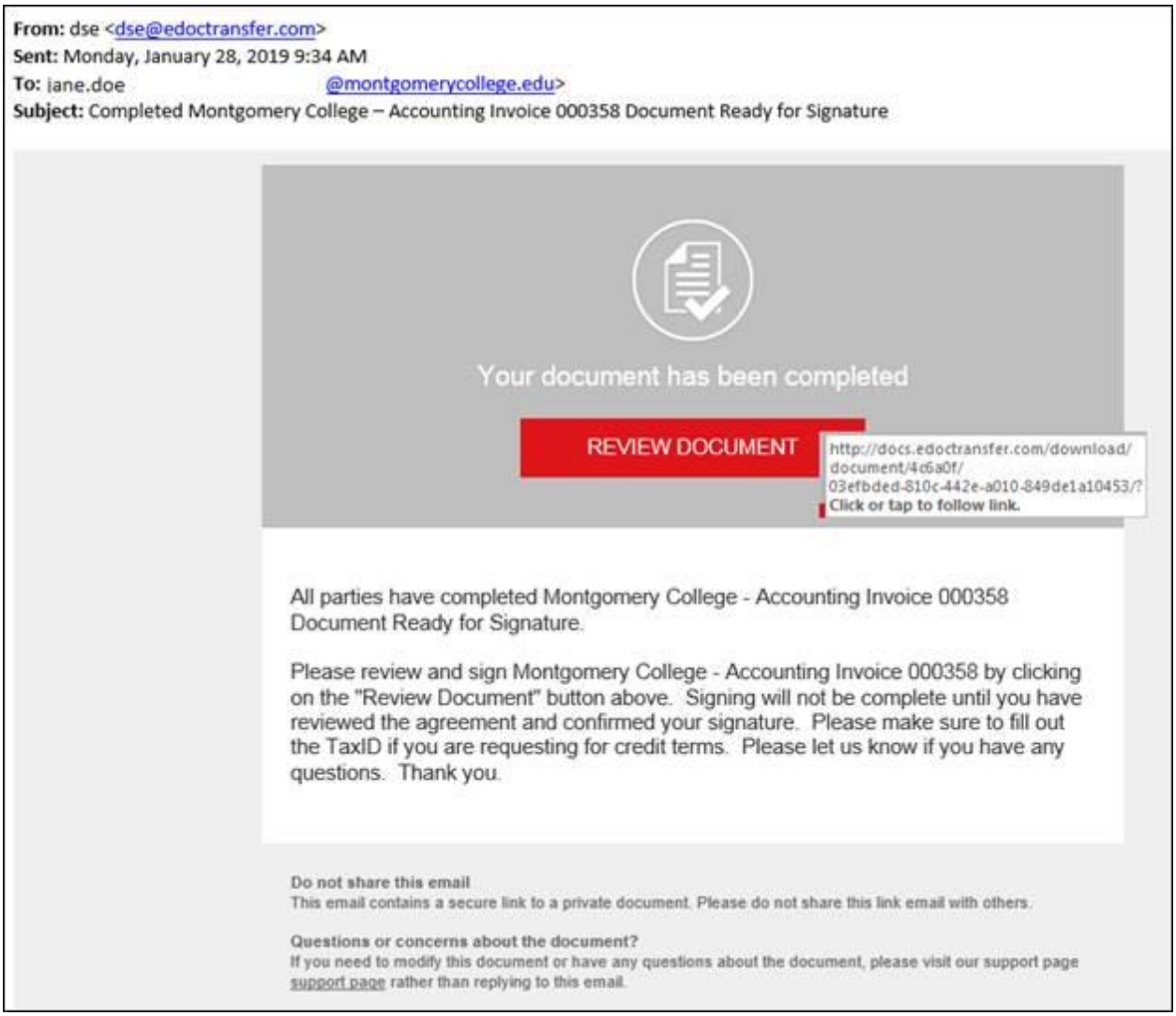
January 2019 Phishing Exercise Recap: Secure Document
February 18, 2019

The Office of Information Technology's (OIT) January 2019 phishing scenario highlighted the real-world threat of "secure document" and "invoice" type emails. Employee reporting took a decline from previous month's scenarios with just 821 employees reporting to the PhishTrap. Employee phishing susceptibility rose with 252 employees clicking on the link within the email. Malicious scammers continue to bait employees with these business-themed emails that appear to be legitimate, because they can be difficult for employees to spot.



To avoid falling victim to "invoice", "secure document", and general phishing emails, OIT recommends all employees:

- Become a “Champion Reporter”. Some departments are higher targets based on their business function, i.e. Financial Aid, Accounts Payable, and Procurement. Report all suspicious emails to the Phishtrap for analysis. IT Security will analyze the content and web links and if found legitimate, will send the email back to you.
- Develop a list of known vendors/business contacts, complete with email addresses and phone numbers, that your department corresponds with and share it with department employees. If a new vendor/contract is established, find out their method of sending invoices and from what domain (example.com) to expect correspondence.
- If you sense something strange or “phishy” about the email, pick up the phone and call the sender. Do not respond back to the sender in an email because the attacker will direct you to complete the request or download the malicious attachment.
- Do NOT click on the links in an email. If you have a business relationship with the sender or an account (MyMC, Amazon.com, your bank, etc.), log in to the account by using the known web address for the account, i.e. montgomerycollege.edu – Access MyMC.
- Enroll in Two-Factor Authentication (2FA) to protect your Office 365 account. Sign up for 2FA, an added layer of security that will help decrease account compromises and identity theft, provide real-time alerts for password protection, and allow you to use your mobile phone, tablet, or landline to easily confirm your login requests. To learn more about 2FA, please visithttps://mcblogs.montgomerycollege.edu/itprojects/2fa.

OIT encourages all employees who need assistance in spotting a phishing email to take the Cybersecurity e-courses within MC Learns. The e-courses are short videos that provide employees with the skills needed to detect malicious emails.